

①9 BUNDESREPUBLIK  
DEUTSCHLAND



DEUTSCHES  
PATENTAMT

⑫ Offenlegungsschrift  
⑩ DE 44 10 459 A 1

⑤1 Int. Cl.<sup>8</sup>:  
H 04 N 1/32  
H 04 N 1/44  
H 04 L 9/32

②1 Aktenzeichen: P 44 10 459.6  
②2 Anmeldetag: 25. 3. 94  
④3 Offenlegungstag: 16. 2. 95

DE 44 10 459 A 1

Mit Einverständnis des Anmelders offengelegte Anmeldung gemäß § 31 Abs. 2 Ziffer 1 PatG

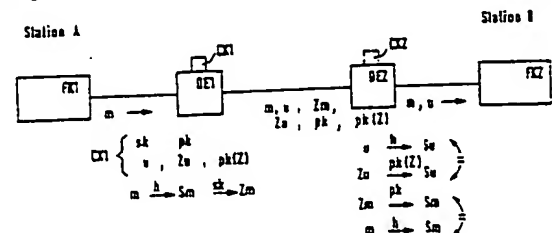
⑦1 Anmelder:  
Siemens AG, 80333 München, DE

⑦2 Erfinder:  
Müller, Horst, 36251 Bad Hersfeld, DE; Römmeling,  
Gerhard, 36251 Ludwigsau, DE

Prüfungsantrag gem. § 44 PatG ist gestellt

⑤4 Elektronisches Unterschriftsverfahren bei der Datenübertragung

⑤7 Die Erfindung betrifft ein elektronisches Unterschriftsverfahren bei der digitalen Übertragung eines Dokumentes, bei dem nacheinander folgende Schritte ausgeführt werden: aus einem zu übertragenden Datensatz (m) des Dokumentes wird eine Dokumenten-Signatur (Sm) gebildet, aus der Signatur (Sm) wird durch ein Kryptieverfahren ein Dokumenten-Zertifikat (Zm) gebildet, ein Datensatz (u) einer persönlichen Unterschrift ist gesichert mit einem Unterschriften-Zertifikat (Zu) abgespeichert, der Dokumenten- und der Unterschriften-Datensatz (m, u), die beiden Zertifikate (Zm, Zu) sowie die dazugehörigen Schlüssel (pk, pk(Z)) werden zu einer Empfangsstation übertragen, dort wird der Unterschriften-Datensatz (u) mit dem Zertifikat (Zu) und anschließend der Dokumenten-Datensatz (m) mit dem Zertifikat (Zm) jeweils durch Berechnung der zugehörigen Signaturen (Su, Sm) auf Unversehrtheit überprüft, und die Datensätze (m, u) des Dokumentes und der Unterschrift werden in lesbarer Form ausgegeben.



DE 44 10 459 A 1

## Beschreibung

Die Erfindung betrifft ein Verfahren zum elektronischen Unterschreiben eines übertragenen Dokumentes.

Durch Verwendung von Fernkopierern können Dokumente auf elektronischem Wege übertragen werden. Solche Dokumente werden aber nicht rechtsverbindlich anerkannt, da sendeseitige Manipulationen nicht ausgeschlossen werden können. Solche Manipulationen sind beispielsweise das Hineinkopieren der Unterschrift einer Person, die das Dokument nie gesehen hat.

Der Erfindung liegt die Aufgabe zugrunde, ein elektronisches Unterschriftenverfahren für ein solches Dokument anzugeben, bei dem die Unterschrift fälschungssicher übertragen wird.

Diese Aufgabe wird erfindungsgemäß durch die im Patentanspruch 1 angegebenen Merkmale gelöst.

Im folgenden wird die Erfindung anhand eines in der Zeichnung dargestellten Ausführungsbeispiels beschrieben.

In der einzigen Figur sind als Blockschaltbild einige Hardwarekomponenten dargestellt, anhand derer die Durchführung des erfindungsgemäßen Verfahrens erläutert wird. Es wird davon ausgegangen, daß ein Dokument von einer Station A zu einer Station B übertragen wird. Hierzu weist die Station A einen Fernkopierer FK1 und die Station B einen Fernkopierer FK2 auf. In der Station A ist weiter eine Datensicherungseinrichtung DE1 und in der Station B eine Datensicherungseinrichtung DE2 vorgesehen. Mit der Datensicherungseinrichtung DE1 ist eine Chipkarte CK1 kontaktiert, so daß ein wechselseitiger Datenaustausch zwischen der Datensicherungseinrichtung DE1 und der Chipkarte CK1 durchgeführt werden kann. Bedarfsweise kann auch auf der Empfangsseite eine Chipkarte CK2 mit der Datensicherungseinrichtung DE2 kontaktiert sein.

In der sendeseitigen Station A wird im Fernkopierer FK1 aus einem nicht dargestellten Dokument ein Dokumenten-Datensatz m gebildet. Dieser Datensatz m wird zur Datensicherungseinrichtung DE1 übertragen und dort vor der Aussendung zur Station B bearbeitet.

Der Urheber des zum Datensatz m gehörenden Dokumentes hat die Chipkarte CK1 mit der Datensicherungseinrichtung DE1 kontaktiert. Diese Chipkarte CK1 ist beispielsweise eine Cryptochipkarte, und der Urheber hat sich durch ein an sich bekanntes Sicherungsverfahren, wie beispielsweise eine PIN (persönliche Identifikationsnummer), ein Paßwort oder ein biometrisches Verfahren gegenüber der Chipkarte CK1 und der Datensicherungseinrichtung DE1 identifiziert.

Der Dokumenten-Datensatz m wird in der Datensicherungseinrichtung DE1 selbst oder in der Chipkarte CK1 signiert, d. h. aus dem Datensatz m wird beispielsweise durch ein Hashverfahren h eine Signatur Sm gewonnen. Zur Durchführung dieser Operation auf der Chipkarte CK1 muß diese eine entsprechende Rechnerkapazität aufweisen.

Auf der Chipkarte CK1 sind beispielsweise ein geheimer und ein öffentlicher Schlüssel sk, pk des Urhebers gespeichert. Diese beiden Schlüssel sk, pk (secret key, public key) und ihre Eigenschaften sind als Bestandteile des sogenannten Public-Key-Verfahrens bekannt.

Weiter ist auf der Chipkarte CK1 die Unterschrift des Urhebers abgespeichert. Diese Unterschrift wurde beispielsweise durch Abtastung der Originalunterschrift des Urhebers gewonnen und in digitalisierter Form als Datensatz u abgespeichert. Auf der Chipkarte CK1 ist ein öffentlicher Schlüssel pk(Z) abgespeichert. Dieser

Schlüssel pk(Z) gehört zu einem geheimen Schlüssel sk(Z), mit dem beispielsweise in einer Zertifizierungsstelle die persönliche Unterschrift gesichert auf der Chipkarte CK1 abgespeichert wurde. Zur Sicherung wurde in der Zertifizierungsstelle aus dem Unterschriften-Datensatz u mit einem Hashverfahren h eine Signatur Su errechnet. Mit dem geheimen Schlüssel sk(Z) der Zertifizierungsstelle wurde aus der Unterschriften-Signatur Su durch ein asymmetrisches Kryptieverfahren ein Zertifikat Zu gebildet. Dieses Zertifikat Zu ist ebenfalls auf der Chipkarte CK1 abgespeichert.

Aus der Signatur Sm des Dokumenten-Datensatzes m wird mit Hilfe des Geheimschlüssels sk des Urhebers durch das asymmetrische Kryptieverfahren ein Zertifikat Zm gewonnen.

Von der Datensicherungseinrichtung DE1 der Station A werden folgende Daten an die Datensicherungseinrichtung DE2 der Station B gesendet: Der Dokumenten-Datensatz m, der Unterschriften-Datensatz u, das Zertifikat Zm und das Zertifikat Zu sowie die zu den geheimen Schlüsseln sk und sk(Z) gehörenden öffentlichen Schlüssel pk und pk(Z) des Urhebers und der Zertifizierungsstelle.

Bei der Verwendung des asymmetrischen Kryptieverfahrens ist der öffentliche Schlüssel pk der zu dem Zertifikat Zm, und der öffentliche Schlüssel pk(Z) der zu dem Zertifikat Zu gehörige Schlüssel, da nur mit ihnen aus den Zertifikaten Zm, Zu die entsprechenden Signaturen Sm, Su zurückgewonnen werden können.

Innerhalb der Datensicherungseinrichtung DE2 oder/und auf der bedarfsweise vorgesehenen Chipkarte CK2 der Station B werden die folgenden Überprüfungen vorgenommen.

In einem ersten Schritt wird der empfangene Unterschriften-Datensatz u mit dem Zertifikat Zu auf Unversehrtheit geprüft. Hierzu wird aus dem Datensatz u über das Hashverfahren h empfangsseitig die Signatur Su gewonnen. Auf einem zweiten Weg wird diese Signatur Su über den öffentlichen Schlüssel pk(Z) aus dem Zertifikat Zu gewonnen. Bei Gleichheit dieser beiden gewonnenen Signaturen Su kann auf die Unversehrtheit der Unterschrift bzw. des zugehörigen Datensatzes u geschlossen werden.

In einem zweiten Schritt wird der empfangene Dokumenten-Datensatz m mit dem Zertifikat Zm auf Unversehrtheit geprüft. Hierzu wird mit dem Hashverfahren h aus dem Datensatz m die Signatur Sm berechnet. Auf einem zweiten Weg wird diese Signatur Sm über den öffentlichen Schlüssel pk aus dem Zertifikat Zm gebildet. Bei Gleichheit dieser beiden Signaturen kann auf die Unversehrtheit des Dokumentes bzw. des zugehörigen Datensatzes m geschlossen werden.

Von der Datensicherungseinrichtung DE2 werden dann die Datensätze m, u des Dokumentes und der Unterschrift an den Fernkopierer Fk2 gegeben. Auf dem Fernkopierer Fk2 kann dann das aus dem Datensatz m reproduzierte Dokument zusammen mit der aus dem Datensatz u reproduzierten Unterschrift ausgedruckt werden. Auch eine schriftliche Darstellung auf einem Bildschirm ist möglich.

Durch das erfindungsgemäße Verfahren ist sichergestellt, daß das empfangsseitig dargestellte, mit einer Unterschrift versehene Dokument mit der Unterschrift des tatsächlichen Urhebers unterzeichnet ist.

## Patentansprüche

## 1. Elektronisches Unterschriftenverfahren bei der di-

3  
gitalen Übertragung eines Dokumentes, bei dem  
nacheinander folgende Schritte ausgeführt werden:  
aus einem zu übertragenden Datensatz (m) des Do-  
kumentes wird eine Dokumenten-Signatur (Sm)  
gebildet, 5  
aus der Signatur (Sm) wird durch ein Kryptiever-  
fahren ein Dokumenten-Zertifikat (Zm) gebildet,  
ein Datensatz (u) einer persönlichen Unterschrift  
ist gesichert mit einem Unterschriften-Zertifikat  
(Zu) abgespeichert, 10  
der Dokumenten- und der Unterschriften-Daten-  
satz (m, u), die beiden Zertifikate (Zm, Zu) sowie die  
dazugehörigen Schlüssel (pk, pk(Z)) werden zu ei-  
ner Empfangsstation übertragen, dort wird der Un-  
terschriften-Datensatz (u) mit dem Zertifikat (Zu) 15  
und anschließend der Dokumenten-Datensatz (m)  
mit dem Zertifikat (Zm) jeweils durch Berechnung  
der zugehörigen Signaturen (Su, Sm) auf Unver-  
sehrtheit überprüft, und die Datensätze (m, u) des  
Dokumentes und der Unterschrift werden in lesba- 20  
rer Form ausgegeben.

2. Elektronisches Unterschriftenverfahren nach An-  
spruch 1, bei dem die Unterschrift als Unterschrif-  
ten-Datensatz (u) in einer Chipkarte (Ck1) gesi-  
chert mit einem Zertifikat (Zu) zusammen mit dem 25  
dazugehörigen Schlüssel (pk(Z)) gespeichert ist.

Hierzu 1 Seite(n) Zeichnungen

30

35

40

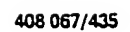
45

50

55

60

65



**Offenlegungsschrift (Laying-open Print)**  
**DE 44 10 459 A1**

Serial No.: P 44 10 459,6  
 Filing date: March 25, 1994  
 Laying-open date: February 16, 1995

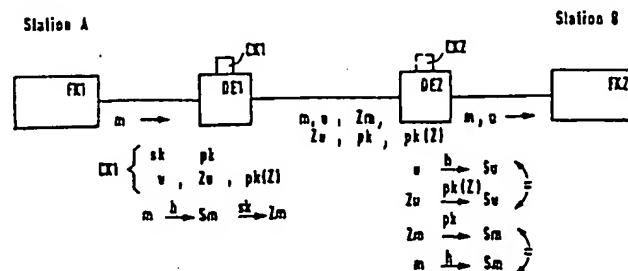
Translation

**Title**

An electronic signature method for data transmission

**Abstract**

This invention refers to an electronic signature method for a digitally transmitted document, in which the following steps are successively carried out: a document signature ( $S_m$ ) is constructed from a document record ( $m$ ) to be transmitted; an encryption method is used to construct a document certificate ( $Z_m$ ) from the signature ( $S_m$ ); a data record ( $u$ ) of a personal signature is secured and stored with a signature certificate ( $Z_u$ ); the document and the signature record ( $m, u$ ), the two the certificates ( $Z_m, Z_u$ ) as well as the pertinent keys ( $pk, pk(Z)$ ) are transmitted to a receiving station, where the signature record ( $u$ ) with the certificate ( $Z_u$ ) and finally the document record ( $m$ ) with the certificate ( $Z_m$ ) are checked for intactness by calculating the corresponding signatures ( $S_u, S_m$ ), and the records ( $m, u$ ) of the document and of the signature are given in legible form.



## Description

This invention refers to a method for electronically signing a transmitted document.

Documents can be electronically transmitted by means of telefax devices. However, such documents are not legally binding, since manipulations on the part of the sender are always possible. For example, a document can be manipulated in such a manner that the signature of a person who has never seen the document is copied onto the document.

The object of this invention is to provide an electronic method of signing a document in such a way that the transmitted signature cannot be forged.

This goal is achieved by the features of the invention given in claim 1.

In the following, the invention is described on the basis of the embodiment shown in the drawing.

In the single figure several hardware components are depicted as a block circuit diagram by means of which components the implementation of the method according to the invention is explained. It is assumed that a document is transmitted from a Station A to a Station B. Station A has a facsimile device (telefax) FK1 and Station B has a facsimile device FK2. Furthermore, Station A is provided with a data securing device DE1, and Station B also has a data securing device DE2. A chip card (smart card) CK1 is contacted with the data securing device DE1, so that a two-way data exchange is made possible between the data securing device DE1 and the chip card CK1. If necessary, a chip card CK2 can also be contacted with the data securing device DE2 on the receiving end.

In the telefax FK1 of transmitting Station A, a document data record  $m$  is constructed from a document not shown here. This record  $m$  is transmitted to the data securing device DE1 and processed there before it is sent on to Station B.

The author of the document belonging to the record  $m$  has brought the chip card CK1 into contact with the data securing device DE1. This chip card can, for example, be a crypto

chip card, and the author has identified himself to the chip card CK1 and the data securing device DE1 by means of a generally known security procedure, such as PIN (personal identification number), a password, or a biometric method .

The data record  $m$  of the document is signed in the data securing device DE1 itself or in the chip card CK1, i.e. a signature  $S_m$  is derived from the record  $m$ , for instance by means of a hash method  $h$ . In order to make it possible to carry out this operation on the chip card CK1, this card has to have an adequate calculating capacity.

For instance, a secret and a public key,  $sk$ ,  $pk$  for the author are stored on the chip card CK1. These two keys  $sk$ ,  $pk$  (secret key, public key) and their characteristics are known as parts of the so-called public key method.

Furthermore, the author's signature is stored on the chip card CK1. This signature was attained, for example, by scanning the author's original signature, and was stored in digital form as a record  $u$ . A public key  $pk(Z)$  is stored on the chip card CK1. This key  $pk(Z)$  belongs to a secret key  $sk(Z)$ , with which, for example, the personal signature can be securely stored on the chip card CK1 in a certification area. As a safety measure, a hash method  $h$  was used in the certification area to calculate a signature  $S_u$  from the signature record  $u$ . With the secret key  $sk(Z)$  of the certification area, a certificate  $Z_u$  was created from the signature  $S_u$  using an asymmetrical encryption method.. This certificate  $Z_u$  is also stored on the chip card CK1.

By using the asymmetrical encryption method, a certificate  $Z_m$  is created from the signature  $S_m$  of the document record  $m$  with the aid of the author's secret key  $sk$ .

From the data securing device DE1 of station A the following data are transmitted to the data securing device DE2 of Station B: the document record  $m$ , the signature record  $u$ , the certificate  $Z_m$  and the certificate  $Z_u$ , as well as the public keys  $pk$  and  $pk(Z)$  of the author and of the certification area, which belong to the secret keys  $sk$  and  $sk(Z)$ .

When the asymmetrical encryption method is used, the public key  $pk$  is the right key for the certificate  $Z_m$ , and the public key  $pk(Z)$  is the right one for certificate  $Z_u$ , since only with these keys can the pertinent signatures  $S_m$  and  $S_u$  be reclaimed from the certificates  $Z_m$  and  $Z_u$ .

The following checks are done within the data securing device DE2 and/or the chip card CK2 of Station B which is provided if necessary.

In a first step, the received signature record  $u$  with the certificate  $Z_u$  is checked to make sure that it is intact. For this purpose the signature  $S_u$  is attained from the record  $u$  using the Hash method  $h$  at the receiving end. Using another method, this signature  $S_u$  is attained via the public key  $pk(Z)$  from the certificate  $Z_u$ . If both of these  $S_u$  signatures are the same, it can be assumed that the signature and the record  $u$  belonging to it are intact.

In a second step, the received document record  $m$  with certificate  $Z_m$  is checked to see if it is intact. For this purpose the hash method  $h$  is used to calculate the signature  $S_m$  from the record  $m$ . A second method is to use the public key  $pk$  to form this signature  $S_m$  from the certificate  $Z_m$ . If both of these signatures are the same, it can be assumed that the document and the record  $m$  belonging to it are intact.

The records  $m$ ,  $u$  of the document and of the signature are then fed to the telefax Fk2 from the data securing device DE2. The document reproduced from the record  $m$  can then be printed on the telefax Fk2 together with the signature reproduced from the record  $u$ . A written depiction on a computer screen is also possible.

The method according to the invention guarantees that the signature on the document which is received corresponds with the signature of the document's actual author.

## Patent Claims

1. An electronic signature method used for the digital transmission of a document, in which the following consecutive steps are taken:  
a document signature ( $S_m$ ) is constructed from a document record ( $m$ ) to be transmitted;  
an encryption method is used to construct a document certificate ( $Z_m$ ) from the signature ( $S_m$ );  
a data record ( $u$ ) of a personal signature is secured and stored with a signature certificate ( $Z_u$ );  
the document and the signature record ( $m, u$ ), the two the certificates ( $Z_m, Z_u$ ) as well as the pertinent keys ( $pk, pk(Z)$ ) are transmitted to a receiving station, where the signature record ( $u$ ) with the certificate ( $Z_u$ ) and finally the document record ( $m$ ) with the certificate ( $Z_m$ ) are checked for intactness by calculating the corresponding signatures ( $S_u, S_m$ ), and the records ( $m, u$ ) of the document and of the signature are given in legible form.
2. The electronic signature method according to claim 1, in which the signature saved in a chip card ( $Ck1$ ) as a signature record ( $u$ ), is stored with a certificate ( $Z_u$ ) together with the pertinent key ( $pk(Z)$ ).